

# RÉDEI SYMBOLS AND ARITHMETICAL MILD PRO-2-GROUPS

JOCHEN GÄRTNER  
MARCH 13, 2013

**ABSTRACT.** Generalizing results of Morishita and Vogel, an explicit description of the triple Massey product for the Galois group  $G_S(2)$  of the maximal 2-extension of  $\mathbb{Q}$  unramified outside a finite set of prime numbers  $S$  containing 2 is given in terms of Rédei symbols. We show that mild pro-2-groups with Zassenhaus invariant 3 occur as Galois groups of the form  $G_S(2)$ . Furthermore, a non-analytic mild fab pro-2-group having only 3 generators is constructed.

## 1. INTRODUCTION

Galois extensions with ramification restricted to finite sets of primes arise naturally in algebraic number theory and arithmetic geometry, e.g. in terms of representations coming from the Galois action on the (étale) cohomology of algebraic varieties defined over number fields. If  $k$  is a number field,  $p$  a prime number and  $S$  is a finite set of primes of  $k$ , we denote by  $k_S(p)$  the maximal pro- $p$ -extension of  $k$  unramified outside  $S$  and by  $G_S(p) = \text{Gal}(k_S(p)|k)$  its Galois group. If  $S$  contains the archimedean primes and the set  $S_p$  of primes of  $k$  lying above  $p$ , the group  $G_S(p)$  is fairly well understood. In particular it has been known that it is of cohomological dimension  $cd\ G_S(p) \leq 2$  (assuming  $k$  is totally imaginary if  $p = 2$ ) and often a duality group. In the *tame case* however, i.e. if  $S \cap S_p = \emptyset$ , the structure of these groups has remained rather mysterious for a long time. Some of the few known results are still conjectural such as the *Fontaine-Mazur conjecture* which predicts that these groups are either finite or not  $p$ -adic analytic.

In his fundamental paper [7], J. Labute could give the first examples of Galois groups of the form  $G_S(p)$  over  $\mathbb{Q}$  in the tame case where  $cd\ G_S(p) = 2$  using the theory of *mild pro- $p$ -groups*. This has been the starting point for more far-reaching studies. We'd like to mention the following remarkable result due to A. Schmidt:

**Theorem** (Schmidt). *Let  $p$  be an odd prime number,  $k$  a number field and  $S$  a finite set of primes of  $k$ . Let  $\mathcal{M}$  be an arbitrary set of primes of  $k$  with Dirichlet density  $\delta(\mathcal{M}) = 0$ . Then there exists a finite set  $S_0$  disjoint from  $S \cup \mathcal{M}$  such that  $cd\ G_{S \cup S_0}(p) = 2$ .*

---

*2010 Mathematics Subject Classification.* 11R34, 12G10, 20E18, 20F05, 55S30.  
*key words and phrases.* Mild pro- $p$ -groups, Massey products, restricted ramification, fab pro- $p$ -groups.

For the precise (and even stronger) statement see [11], Th.1.1. Note that in the above theorem the set  $S_0$  can always be chosen to be disjoint from  $S_p$ .

As an important ingredient in the proof of the above theorem, using results of J. Labute, A. Schmidt showed that a finitely presented pro- $p$ -group  $G$  is mild (and hence of cohomological dimension  $cd\ G = 2$ ) if the cohomology group  $H^1(G, \mathbb{F}_p)$  admits a direct sum decomposition  $H^1(G, \mathbb{F}_p) = U \oplus V$  such that the cup-product  $\cup : H^1(G, \mathbb{F}_p) \otimes H^1(G, \mathbb{F}_p) \rightarrow H^2(G, \mathbb{F}_p)$  maps  $U \otimes V$  surjectively onto  $H^2(G, \mathbb{F}_p)$  and is identically zero on  $V \otimes V$ . Note that this cup-product being surjective is equivalent to  $G$  having a minimal system of defining relations which are linearly independent modulo the third step of the *Zassenhaus filtration*. In [2], the author generalizes Schmidt's cup-product criterion to finitely presented pro- $p$ -groups with arbitrary *Zassenhaus invariant* using higher *Massey products*. However, it does not follow from Schmidt's result that mild pro- $p$ -groups with Zassenhaus invariant  $> 2$  occur as Galois groups of the form  $G_S(p)$ . The goal of this paper is to give an affirmative answer to this question. More precisely, we will prove the following result in the case  $k = \mathbb{Q}, p = 2$ :

**Theorem (Th.4.9).** *Let  $S = \{2, l_1, \dots, l_n\}$  for some  $n \geq 1$  and prime numbers  $l_i \equiv 9 \pmod{16}$ ,  $i = 1, \dots, n$ , such that the Legendre symbols satisfy*

$$\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n, \quad i \neq j.$$

*Then  $G_S(2) = \text{Gal}(\mathbb{Q}_S(2)|\mathbb{Q})$  is a mild pro-2-group with generator rank  $n + 1$ , relation rank  $n$  and Zassenhaus invariant  $\mathfrak{z}(G) = 3$ .*

We will show that the triple Massey product for the group  $G_S(2)$  is amenable to an explicit description via *Rédei symbols*. Furthermore, we consider certain *fab* quotients of the groups  $G_S(2)$  and give an explicit description of their triple Massey products, cf. Th.5.2. This will enable us to construct an explicit example of a mild, non-analytic *fab* pro-2-group with Zassenhaus invariant 3.

**Acknowledgements:** Parts of the results in this article are contained in the author's PhD thesis. The author likes to thank Kay Wingberg for his guidance and great support and to Alexander Schmidt and Denis Vogel for helpful suggestions. Further thanks go to Hugo Chapdelaine and Claude Levesque for providing a relevant reference concerning the 2-class group of a quadratic number field.

## 2. REVIEW OF MASSEY PRODUCTS IN THE COHOMOLOGY OF PRO- $p$ -GROUPS

In this section we recall the definition and properties of higher Massey products for group cohomology of pro- $p$ -groups. We will not give any proofs and refer the reader to the existing literature (e.g. see [5] and [12]).

Let  $p$  be a prime number. With a view towards our applications, for a pro- $p$ -group  $G$  we consider the trivial  $G$ -module  $\mathbb{F}_p$  only and set

$$H^i(G) = H^i(G, \mathbb{F}_p), \quad h^i = \dim_{\mathbb{F}_p} H^i(G).$$

By  $\mathcal{C}^*(G) = \mathcal{C}^*(G, \mathbb{F}_p)$  we denote the standard inhomogeneous cochain complex (e.g. see [9], Ch.I, §2).

**Definition 2.1.** Let  $n \geq 2$  and  $\alpha_1, \dots, \alpha_n \in H^1(G)$ . We say that the  $n$ -th Massey product  $\langle \alpha_1, \dots, \alpha_n \rangle_n$  is defined if there is a collection

$$\mathcal{A} = \{a_{ij} \in \mathcal{C}^1(G) \mid 1 \leq i, j \leq n, (i, j) \neq (1, n)\}$$

(called a *defining system* for  $\langle \alpha_1, \dots, \alpha_n \rangle_n$ ), such that the following conditions hold:

- (i)  $a_{ii}$  is a representative of the cohomology class  $\alpha_i$ ,  $1 \leq i \leq n$ .
- (ii) For  $1 \leq i < j \leq n$ ,  $(i, j) \neq (1, n)$  it holds that

$$\partial^2(a_{ij}) = \sum_{l=i}^{j-1} a_{il} \cup a_{(l+1)j}$$

where  $\partial^2$  denotes the coboundary operator  $\partial^2 : \mathcal{C}^1(G) \longrightarrow \mathcal{C}^2(G)$ . If  $\mathcal{A}$  is a defining system for  $\langle \alpha_1, \dots, \alpha_n \rangle_n$ , the 2-cochain

$$b_{\mathcal{A}} = \sum_{l=1}^{n-1} a_{1l} \cup a_{(l+1)n}$$

is a cocycle and we denote its class in  $H^2(G)$  by  $\langle \alpha_1, \dots, \alpha_n \rangle_{\mathcal{A}}$ . We set

$$\langle \alpha_1, \dots, \alpha_n \rangle_n = \bigcup_{\mathcal{A}} \langle \alpha_1, \dots, \alpha_n \rangle_{\mathcal{A}}$$

where  $\mathcal{A}$  runs over all defining systems. The Massey product  $\langle \alpha_1, \dots, \alpha_n \rangle_n$  is called *uniquely defined* if  $\#\langle \alpha_1, \dots, \alpha_n \rangle_n = 1$ . We say that the  $n$ -th Massey product is *uniquely defined for  $G$*  if  $\langle \alpha_1, \dots, \alpha_n \rangle_n$  is uniquely defined for all  $\alpha_1, \dots, \alpha_n \in H^1(G)$ .

The 2-fold Massey product is uniquely defined given by the cup-product  $\cup : H^1(G) \times H^1(G) \rightarrow H^2(G)$ . If this cup-product is identically zero, the triple Massey product is uniquely defined. More generally, if  $n \geq 2$  and the  $k$ -th Massey product is uniquely defined and identically zero for all  $k < n$ , the  $n$ -th Massey product is also uniquely defined and yields a multilinear map of  $\mathbb{F}_p$ -vector spaces

$$\langle \cdot, \dots, \cdot \rangle_n : H^1(G)^n \longrightarrow H^2(G).$$

**Remark 2.2.** The  $n$ -th Massey products commute with inflation, restriction and corestriction homomorphisms provided they are uniquely defined. In fact, this follows directly from their definition and the functoriality properties of the cup-product on the level of cochains. Furthermore, generalizing the anti-commutativity of the cup-product, Massey products satisfy certain *shuffle identities*, cf. [2], Prop. 4.8.

Now assume that the pro- $p$ -group  $G$  is finitely generated, i.e.  $h^1(G) < \infty$ . It has been remarked by H. Koch that higher Massey products are closely related to structure of relation systems of  $G$ . In order to make this connection precise,

we need the definition of the *Zassenhaus filtration*. Let  $\Omega_G$  denote the complete group algebra

$$\Omega_G = \mathbb{F}_p[[G]] = \varprojlim_U \mathbb{F}_p[G/U]$$

where  $U$  runs through the open normal subgroups of  $G$ . By  $I_G \subseteq \Omega_G$  we denote the *augmentation ideal* of  $G$ , i.e. the kernel of the canonical *augmentation map*

$$\begin{aligned} \Omega_G &\longrightarrow \mathbb{F}_p, \\ g &\longmapsto 1, \quad g \in G. \end{aligned}$$

The *Zassenhaus filtration*  $(G_{(n)})_{n \in \mathbb{N}}$  of  $G$  is given by

$$G_{(n)} = \{g \in G \mid g - 1 \in I_G^n\}.$$

The groups  $G_{(n)}, n \in \mathbb{N}$  form a system of neighborhoods  $1 \in G$  consisting of open normal subgroups.

Let

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

be a minimal presentation of  $G$ , i.e.  $F$  is a free pro- $p$ -group on generators  $x_1, \dots, x_d$ ,  $d = h^1(G)$ . By  $\chi_i = x_i^*$  we denote the basis of the  $\mathbb{F}_p$ -vector space  $H^1(F) = H^1(G)$  dual to the  $x_i$ . By the Hochschild-Serre spectral sequence, we have the transgression isomorphism

$$tg : H^1(R)^G \xrightarrow{\sim} H^2(G).$$

Hence, every element  $r \in R$  gives rise to a *trace map*

$$\begin{aligned} tr_r : H^2(G) &\longrightarrow \mathbb{F}_p, \\ \varphi &\longmapsto (tg^{-1}\varphi)(r). \end{aligned}$$

If  $r_i \in R, i \in I$  is a minimal system of defining relations for  $G$  (i.e. a minimal system of generators of  $R$  as closed normal subgroup of  $F$ ), then  $\{tr_{r_i}, i \in I\}$  is a basis of the dual space  $H^2(G)^\vee$ . Furthermore, note that for the free pro- $p$ -group  $F$  we have a topological isomorphism

$$\Omega_F \xrightarrow{\sim} \mathbb{F}_p\langle\langle X \rangle\rangle, \quad x_i \longmapsto 1 + X_i$$

where  $\mathbb{F}_p\langle\langle X \rangle\rangle$  denotes the  $\mathbb{F}_p$ -algebra of formal power series in the non-commuting indeterminates  $X = \{X_1, \dots, X_d\}$ . Let  $\psi : F \hookrightarrow \mathbb{F}_p\langle\langle X \rangle\rangle$  denote the composite of the map  $F \hookrightarrow \Omega_F, f \mapsto f - 1$  with the above isomorphism, mapping  $F$  into the augmentation ideal of  $\mathbb{F}_p\langle\langle X \rangle\rangle$  and the generator  $x_i$  to  $X_i$ .

**Definition 2.3.** The element  $\psi(f)$  is called *Magnus expansion* of  $f \in F$ . For any multi-index  $I = (i_1, \dots, i_k)$ ,  $1 \leq i_j \leq d$  of height  $d$  we set  $X_I = X_{i_1} \cdots X_{i_k}$  and define the numbers  $\varepsilon_{I,p}(f)$  by

$$\psi(f) = \sum_I \varepsilon_{I,p}(f) X_I$$

where  $I$  runs over all multi-indices of height  $d$ .

By definition  $f \in F_{(n)}$  holds if and only if  $\varepsilon_{I,p}(f) = 0$  for all multi-indices  $I = (i_1, \dots, i_k)$  of length  $k < n$ . The following result proven independently by M. Morishita ([8], Th.2.2.2) and D. Vogel ([12], Prop.1.2.6) generalizes a well-known connection between the cup-product and relations modulo  $F_{(3)}$  to higher degrees:

**Theorem 2.4.** *Let  $G$  be a finitely presented pro- $p$ -group and*

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

*be a minimal presentation. Assume that  $R \subseteq F_{(n)}$  for some  $n \geq 2$ . Then for all  $2 \leq k \leq n$  the  $k$ -fold Massey product*

$$\langle \cdot, \dots, \cdot \rangle_k : H^1(G)^k \longrightarrow H^2(G)$$

*is uniquely defined. Furthermore, for all multi-indices  $I$  of height  $d$  and length  $2 \leq |I| \leq n$  and for all  $r \in R$  we have the equality*

$$\varepsilon_{I,p}(r) = (-1)^{|I|-1} \text{tr}_r \langle \chi_I \rangle_{|I|}$$

*where for  $I = (i_1, \dots, i_k)$  we have set  $\chi_I = (\chi_{i_1}, \dots, \chi_{i_k}) \in H^1(G)^k$ . In particular, for  $1 < k < n$  the  $k$ -fold Massey product on  $H^1(G)$  is identically zero.*

The above result gives rise to the following

**Definition 2.5.** Let  $G$  be a finitely generated pro- $p$ -group. We define the *Zassenhaus invariant*  $\mathfrak{z}(G) \in \mathbb{N} \cup \{\infty\}$  to be the supremum of all natural numbers  $n$  satisfying one of the following equivalent conditions:

- (i) If  $1 \rightarrow R \rightarrow F \rightarrow G \rightarrow 1$  is a minimal presentation of  $G$ , then  $R \subseteq F_{(n)}$ .
- (ii) The  $k$ -fold Massey product  $H^1(G)^k \rightarrow H^2(G)$  is uniquely defined and identically zero for  $2 \leq k < n$ .

Note that  $\mathfrak{z}(G) = \infty$  if and only if  $G$  is free. Now assume that  $G$  is *finitely presented*, i.e.  $h^1(G), h^2(G) < \infty$ . Let

$$G = \langle x_1, \dots, x_d \mid r_1, \dots, r_m \rangle$$

be a minimal presentation of  $G$ , i.e.  $G = F/R$  where  $F$  is the free pro- $p$ -group on generators  $x_1, \dots, x_d$ ,  $d = h^1(G)$  and  $R$  is generated by  $r_1, \dots, r_m$  as closed normal subgroup of  $F$ . Let  $\rho_i$ ,  $i = 1, \dots, m$  denote the initial form of  $r_i$  in the graded  $\mathbb{F}_p$ -Lie algebra

$$\text{gr } F = \bigoplus_{n \geq 1} F_{(n)} / F_{(n+1)}.$$

The map  $\psi : F \hookrightarrow \mathbb{F}_p \langle\langle X \rangle\rangle$  induces an inclusion (of  $\mathbb{F}_p$ -Lie algebras)

$$\text{gr } F \subseteq \text{gr } \mathbb{F}_p \langle\langle X \rangle\rangle = \bigoplus_{n \geq 0} \mathbb{F}_p \langle\langle X \rangle\rangle_n / \mathbb{F}_p \langle\langle X \rangle\rangle_{n+1} = \mathbb{F}_p \langle X \rangle$$

where  $\mathbb{F}_p \langle\langle X \rangle\rangle_n \subseteq \mathbb{F}_p \langle\langle X \rangle\rangle$  denotes the two-sided ideal of power series of degree  $\geq n$  and  $\mathbb{F}_p \langle X \rangle$  is the free associative  $\mathbb{F}_p$ -algebra on  $X = \{X_1, \dots, X_d\}$ . The presentation  $G = \langle x_1, \dots, x_d \mid r_1, \dots, r_m \rangle$  is called *strongly free*, if the images of  $\rho_i$  in  $\mathbb{F}_p \langle X \rangle$  form a *strongly free sequence*. (The notion of strongly free sequences is due to D. Anick, see [2], Def.2.7 for a definition.) We say that  $G$  is a *mild*

*pro-p-group* (with respect to the Zassenhaus filtration) if it possesses a strongly free presentation.

**Remark 2.6.** The theory of mild groups has originally been developed by J. Labute in the case of discrete groups and later applied to *pro-p*-groups in [7]. Note that they can be defined with respect to different filtrations such as weighted lower *p*-central series and weighted Zassenhaus filtrations.

The main properties of mild *pro-p*-groups is given by the following

**Theorem 2.7.** *Let  $G$  be a mild *pro-p*-group and  $G = \langle x_1, \dots, x_d \mid r_1, \dots, r_m \rangle$  a strongly free presentation. Then  $h^2(G) = m$ ,  $G$  is of cohomological dimension  $\text{cd } G = 2$  and if  $m \neq d - 1$  it is not *p*-adic analytic.*

For a proof we refer to [2], Th.2.12 which is a slight generalization of [7], Th.5.1.

In order to find arithmetical examples of mild *pro-p*-groups  $G$  with Zassenhaus invariant  $\mathfrak{z}(G) = 3$ , we will make use of the following result, cf. [2] Th.4.9:

**Theorem 2.8.** *Let  $p$  be a prime number and  $G$  a finitely presented *pro-p*-group with  $n = \mathfrak{z}(G) < \infty$ . Assume that  $H^1(G)$  admits a decomposition  $H^1(G) = U \oplus V$  as  $\mathbb{F}_p$ -vector space such that for some natural number  $e$  with  $1 \leq e \leq n - 1$  the  $n$ -fold Massey product  $\langle \cdot, \dots, \cdot \rangle_n : H^1(G)^n \longrightarrow H^2(G)$  satisfies the following conditions:*

- (a)  $\langle \xi_1, \dots, \xi_n \rangle_n = 0$  for all tuples  $(\xi_1, \dots, \xi_n) \in H^1(G)^n$  such that  $\#\{i \mid \xi_i \in V\} \geq n - e + 1$ .
- (b)  $\langle \cdot, \dots, \cdot \rangle_n$  maps

$$U^{\otimes e} \otimes V^{\otimes n-e}$$

*surjectively onto  $H^2(G)$ .*

*Then  $G$  is mild (with respect to the Zassenhaus filtration).*

### 3. TOTALLY REAL PRO-2-EXTENSIONS WITH WILD RAMIFICATION

As has been remarked in the introduction, the theory of mild *pro-p*-groups has had a great impact in the study of *pro-p*-extensions of number fields with restricted ramification. From the group-theoretical point of view, an important tool in the proof of Schmidt's theorem [11], Th.1.1 is the *cup-product criterion*. The groups  $G_{S \cup S_0}(p)$  that are obtained by enlarging the set  $S$  and satisfy  $\text{cd } G_{S \cup S_0}(p) = 2$  have Zassenhaus invariant  $\mathfrak{z}(G_{S \cup S_0}(p)) = 2$ .

On the other hand, for sets of primes  $S$  such that  $\mathfrak{z}(G_S(p)) \geq 3$  there have been no known examples where the cohomological dimension of  $G_S(p)$  is finite. Having the generalized criterion 2.8 using higher Massey products at hand, the question naturally arises whether mild *pro-p*-groups with Zassenhaus invariant at least 3 arise as arithmetically defined Galois groups, i.e. (quotients of) groups of the form  $G_S(p)$ . In the following we give a positive answer in the case of *pro-2*-extensions of the rationals.

We fix the following notation: For a finite set  $S$  of primes of  $\mathbb{Q}$ , we denote by  $\mathbb{Q}_S(2)|\mathbb{Q}$  the maximal *pro-2*-extension of  $\mathbb{Q}$  unramified outside  $S$  and denote by  $G_S(2) = \text{Gal}(\mathbb{Q}_S(2)|\mathbb{Q})$  its Galois group. Let  $\infty$  denote the infinite prime of  $\mathbb{Q}$ .

We consider the local extension  $\mathbb{C}|\mathbb{R}$  as being ramified, i.e. if  $\infty \notin S$ ,  $\mathbb{Q}_S(2)|\mathbb{Q}$  is totally real.

An explicit construction of mild groups of the form  $G_S(2)$  with Zassenhaus invariant 3 amounts to giving an arithmetic description of the triple Massey product

$$\langle \cdot, \cdot, \cdot \rangle_3 : H^1(G_S(2)) \times H^1(G_S(2)) \times H^1(G_S(2)) \longrightarrow H^2(G_S(2)),$$

or, equivalently, of the relation structure of  $G_S(2)$  modulo the fourth step of the Zassenhaus filtration. Such a description has been given by M. Morishita and D. Vogel in terms of *Rédei symbols* in the case where  $S$  is a finite set consisting of the infinite prime and prime numbers  $l_1, \dots, l_n \equiv 1 \pmod{4}$  such that the Legendre symbols  $\left(\frac{l_i}{l_j}\right)$  are pairwise trivial. However, for such sets  $S$  the extension  $\mathbb{Q}_S(2)$  is always totally imaginary and therefore the Galois group  $G_S(2)$ , having 2-torsion, satisfies  $cd\ G_S(2) = \infty$ . Consequently, in order to construct mild examples, we have to remove ramification at  $\infty$ .

By results of I.R. Šafarevič and H. Koch, there is a presentation for  $G_S(2)$  in terms of generators and relations of local Galois groups provided that the *Šafarevič-Tate group*  $\text{III}_S(2)$  given by the exact sequence

$$0 \longrightarrow \text{III}_S(2) \longrightarrow H^2(G_S(2), \mathbb{F}_2) \longrightarrow \prod_{l \in S} H^2(G_l(2), \mathbb{F}_2)$$

vanishes where  $G_l(2)$  denotes the Galois group of the maximal pro-2-extension of  $\mathbb{Q}_l$  if  $l$  is a finite prime and  $G_l(2) = \text{Gal}(\mathbb{C}|\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$  if  $l = \infty$ . We have a natural inclusion  $\text{III}_S(2) \hookrightarrow \text{B}_S(2)$  into the Pontryagin dual  $\text{B}_S(2) = (V_S(2))^\vee$  of the *Kummer group*

$$V_S(2) = \{x \in \mathbb{Q}^\times \mid x \in U_l \mathbb{Q}_l^{\times 2} \text{ if } l \notin S, x \in \mathbb{Q}_l^{\times 2} \text{ if } l \in S\} / \mathbb{Q}^{\times 2}$$

where  $U_l = \mathbb{Z}_l^\times$  if  $l \neq \infty$  and  $U_l = \mathbb{R}^\times$  if  $l = \infty$ . Noting that

$$V_\emptyset(2) = \{\pm 1\} \mathbb{Q}^{\times 2} / \mathbb{Q}^{\times 2} \cong \{\pm 1\},$$

we see that if  $\infty \notin S$  then  $V_S(2) = 1$  if and only if  $S$  contains 2 or a prime  $l \equiv 3 \pmod{4}$ . However if  $S$  contains more than one prime  $l \equiv 3 \pmod{4}$ , we have  $\mathfrak{z}(G_S(2)) = 2$  since by quadratic reciprocity there are non-trivial Legendre symbols. If  $S$  contains exactly one prime  $l \equiv 3 \pmod{4}$  then it can be shown that  $G_S(2)$  is never mild. Consequently in the following we consider a finite  $S$  of rational primes such that  $2 \in S, \infty \notin S$ . Recall that for a pro-2-group  $G$  we set  $H^i(G) = H^i(G, \mathbb{F}_2)$ ,  $h^i(G) = \dim_{\mathbb{F}_2} H^i(G)$ . We start with the following

**Proposition 3.1.** *Let  $S = \{2, l_1, \dots, l_n\}$  for some  $n \geq 1$  and odd prime numbers  $l_1, \dots, l_n$ . Then the pro-2-group  $G_S(2)$  has cohomological dimension  $cd\ G_S(2) = 2$  and the generator and relation ranks satisfy*

$$h^1(G_S(2)) = n + 1, \quad h^2(G_S(2)) = n.$$

*Furthermore, the abelianization  $G_S(2)^{ab}$  is infinite.*

*Proof.* Since by assumption  $2 \in S, \infty \notin S$ , [9] Th.10.6.1 yields  $cd\ G_S(2) \leq 2$  and  $\chi_2(G_S(2)) = 0$  where  $\chi_2(G_S(2)) = \sum_{i \geq 0} (-1)^i h^i(G_S(2))$  denotes the Euler-Poincaré characteristic of  $G_S(2)$ . Since  $\text{B}_S(\mathbb{Q}) = (V_S(\mathbb{Q}))^\vee$  is trivial,

the general formula [9], Th.10.7.12 yields  $h^1(G_S(2)) = 1 + n$  and thus also the second formula  $h^2(G_S(2)) = n$  holds. In particular,  $cd\ G_S(2) = 2$  and we have  $h^2(G_S(2)) < h^1(G_S(2))$ , which implies the infiniteness of  $G_S(2)^{ab}$ . Alternatively, the infiniteness of  $G_S(2)^{ab}$  also follows directly from the fact that  $\mathbb{Q}_S(2)$  contains the cyclotomic  $\mathbb{Z}_2$ -extension of  $\mathbb{Q}$ .  $\square$

We will now determine necessary and sufficient conditions for  $\mathfrak{z}(G_S(2)) > 2$ . By the results of Šafarevič and Koch, we have a minimal presentation of groups of the form  $G_S(p)$  with the relations determined modulo the third step of the Zassenhaus filtration. Choosing generators of inertia subgroups of  $G_S(2)$  and appropriate relations of corresponding local Galois groups, this is made possible by the interplay of local and global class field theory. For the latter we make use of the idèlic formulation throughout, cf. [9], Ch.VIII.

The following lemma is well-known. However, as has been pointed out to the author by D. Vogel, the main reference [3] contains a sign error in the case  $l = 2$ , therefore we included the statement here:

**Lemma 3.2.** *Let  $l$  be a prime number and  $G_l(2)$  be the Galois group of the maximal 2-extension  $\mathbb{Q}_l(2)$  of  $\mathbb{Q}_l$ . Let  $\mathcal{T}_l(2) \subseteq G_l(2)$  denote the inertia group of  $G_l(2)$ .*

- (i) *If  $l \neq 2$ , then  $\mathcal{T}_l(2) \cong \mathbb{Z}_2$  and  $G_l(2)$  is a pro-2-group with two generators  $\sigma, \tau$  satisfying the relation*

$$\tau^{l-1}[\tau^{-1}, \sigma^{-1}] = 1$$

*where  $\sigma$  denotes an arbitrary lift of the Frobenius automorphism of the maximal unramified 2-extension of  $\mathbb{Q}_l$  and  $\tau$  is an arbitrary generator of  $\mathcal{T}_l$ .*

- (ii) *If  $l = 2$ , let  $\sigma, \tau, \tilde{\tau}$  be arbitrary elements of  $G_2(2)$  such that*

$$\begin{aligned} \sigma &\equiv (2, \mathbb{Q}_2(2)^{ab} | \mathbb{Q}_2) \pmod{[G_2(2), G_2(2)]}, \\ \tau &\equiv (5, \mathbb{Q}_2(2)^{ab} | \mathbb{Q}_2) \pmod{[G_2(2), G_2(2)]}, \\ \tilde{\tau} &\equiv (-1, \mathbb{Q}_2(2)^{ab} | \mathbb{Q}_2) \pmod{[G_2(2), G_2(2)]} \end{aligned}$$

*where  $(\cdot, \mathbb{Q}_2(2)^{ab} | \mathbb{Q}_2)$  denotes the local norm residue symbol. Then  $\sigma$  is a lift of the Frobenius automorphism of the maximal unramified 2-extension of  $\mathbb{Q}_2$ ,  $\tau, \tilde{\tau} \in \mathcal{T}_2(2)$  and  $\{\sigma, \tau, \tilde{\tau}\}$  form a minimal system of generators of  $G_2(2)$ . We have  $h^2(G_2(2)) = 1$  and in a minimal presentation*

$$1 \longrightarrow R \longrightarrow F \longrightarrow G_2(2) \longrightarrow 1$$

*with preimages  $s, t, \tilde{t}$  of  $\sigma, \tau, \tilde{\tau}$  respectively, the single relation  $r$  can be chosen in the form*

$$r \equiv \tilde{t}^2[t, s] \pmod{F_{(3)}}.$$

*Furthermore,  $\tau$  and  $\tilde{\tau}$  generate  $\mathcal{T}_2(2)$  as a normal subgroup of  $G_2(2)$ .*



*Proof.* The first statement is a special case of [3], Th.10.2. For the second statement note that for  $\pi = 2$ ,  $\alpha_0 = 5$ ,  $\alpha_1 = -1$  the set  $\{\pi, \alpha_0, \alpha_1\}$  is a basis of  $\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2}$  satisfying the conditions of [3], Lemma 10.10. (Note that with a view to the correctness of the following Th.10.12 loc. cit., this lemma contains a sign error in (iv); the condition  $(\alpha_1, \pi) = -1$  has to be replaced by  $(\alpha_1, \pi) = 1$ , which holds for the above choice.) Then [3], Th.10.12 yields (ii). In fact, in order to see that  $\tau, \tilde{\tau}$  generate  $\mathcal{T}_2(2)$  as a normal subgroup of  $G_2(2)$ , let  $\Gamma_2(2) = G_2(2)/\mathcal{T}_2(2)$  and consider the Hochschild-Serre exact sequence

$$0 \longrightarrow H^1(\Gamma_2(2)) \longrightarrow H^1(G_2(2)) \longrightarrow H^1(\mathcal{T}_2(2))^{\Gamma_2(2)} \longrightarrow H^2(\Gamma_2(2)),$$

which yields  $\dim_{\mathbb{F}_2} H^1(\mathcal{T}_2(2))^{\Gamma_2(2)} = 2$  since  $h^1(\Gamma_2(2)) = 1$ ,  $h^2(\Gamma_2(2)) = 0$ . The elements  $\tau, \tilde{\tau} \in \mathcal{T}_2(2)$  are contained in a minimal system of generators of  $G_2(2)$ , hence they are linearly independent modulo  $\mathcal{T}_2(2)^2[G_2(2), \mathcal{T}_2(2)]$ . Now the claim follows by reason of dimension.  $\square$

We return to the global Galois group  $G_S(2)$ . Let  $S = \{l_0, l_1, \dots, l_n\}$  where  $l_0 = 2$  and  $l_i$  is an odd prime number for  $i = 1, \dots, n$ . We fix the following notations:

- (i) For each  $0 \leq i \leq n$  let  $\mathfrak{l}_i$  denote a fixed prime of  $\mathbb{Q}_S(2)$  above  $l_i$ .
- (ii) For  $1 \leq i \leq n$  let  $\hat{l}_i$  denote the idèle of  $\mathbb{Q}$  whose  $l_i$ -component equals  $l_i$  and all other components are 1 and let  $\hat{g}_i$  denote the idèle whose  $l_i$ -component equals  $g_i$  for a primitive root  $g_i$  modulo  $l_i$  and all other components are 1.
- (iii) For  $i = 0$  let  $\hat{l}_0, \hat{g}_0, \hat{g}'_0$  denote the idèles of  $\mathbb{Q}$  whose 2-components are 2, 5 and  $-1$  respectively and all other components are 1.

For  $0 \leq i \leq n$  we choose an element  $\sigma_i \in G_S(2)$  with the following properties:

- (i)  $\sigma_i$  is a lift of the Frobenius automorphism of  $\mathfrak{l}_i$  with respect to the maximal subextension of  $\mathbb{Q}_S(2)|\mathbb{Q}$  in which  $\mathfrak{l}_i$  is unramified;
- (ii) the restriction of  $\sigma_i$  to the maximal abelian subextension  $\mathbb{Q}_S(2)^{ab}|\mathbb{Q}$  of  $\mathbb{Q}_S(2)|\mathbb{Q}$  equals  $(\hat{l}_i, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$  where  $(\cdot, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$  denotes the global norm residue symbol.

For  $1 \leq i \leq n$  we denote by  $T_{\mathfrak{l}_i} \subseteq G_S(2)$  the inertia subgroup of  $\mathfrak{l}_i$  and choose an element  $\tau_i \in T_{\mathfrak{l}_i}$ , such that

- (i)  $\tau_i$  generates  $T_{\mathfrak{l}_i}$ ;
- (ii) the restriction of  $\tau_i$  to  $\mathbb{Q}_S(2)^{ab}|\mathbb{Q}$  equals  $(\hat{g}_i, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$ .

Finally, let  $\tau_0, \tilde{\tau}_0$  denote two elements of the inertia subgroup  $T_{\mathfrak{l}_0} \subseteq G_S(2)$  of  $\mathfrak{l}_0$  such that

- (i)  $\tau_0, \tilde{\tau}_0$  generate  $T_{\mathfrak{l}_0}$  as a normal subgroup of the decomposition group  $G_{\mathfrak{l}_0} \subseteq G_S(2)$  of  $\mathfrak{l}_0$ ;
- (ii) the restriction of  $\tau_0$  to  $\mathbb{Q}_S(2)^{ab}|\mathbb{Q}$  equals  $(\hat{g}_0, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$  and the restriction of  $\tilde{\tau}_0$  to  $\mathbb{Q}_S(2)^{ab}|\mathbb{Q}$  equals  $(\hat{g}'_0, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$ .

The existence of the elements  $\sigma_i, \tau_i, \tilde{\tau}_0$  follows by class field theory and the structure result 3.2 of local pro-2-Galois groups.

**Definition 3.3.** For  $1 \leq i, j \leq n$ ,  $i \neq j$  we define the *linking number*  $a_{i,j} \in \mathbb{F}_2$  by

$$a_{i,j} = \begin{cases} 1, & \text{if } \left(\frac{l_i}{l_j}\right)_2 = -1, \\ 0, & \text{else.} \end{cases}$$

Furthermore, for  $1 \leq i \leq n$  we define the numbers  $a_{i,0}, \tilde{a}_{i,0} \in \mathbb{F}_2$  by

$$\begin{aligned} a_{i,0} &= \begin{cases} 1, & \text{if } l_i \equiv 3, 5 \pmod{8}, \\ 0, & \text{else} \end{cases} \quad \text{and} \\ \tilde{a}_{i,0} &= \begin{cases} 1, & \text{if } l_i \equiv 3, 7 \pmod{8}, \\ 0, & \text{else.} \end{cases} \end{aligned}$$

We can now give the desired description of the group  $G_S(2)$  in terms of generators and relations:

**Proposition 3.4.** Let  $S = \{l_0, \dots, l_n\}$  where  $l_0 = 2$  and  $l_1, \dots, l_n$  are odd prime numbers. Furthermore, let  $F$  be the free pro-2-group on the  $n+1$  generators  $x_0, \dots, x_n$ . Then  $G_S(2)$  admits a minimal presentation

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G_S(2) \longrightarrow 1$$

where  $\pi$  maps  $x_i$  to  $\tau_i$  for  $0 \leq i \leq n$ . Let  $y_i$  denote a preimage of  $\sigma_i$  under  $\pi$ , then a minimal generating set of  $R$  as closed normal subgroup of  $F$  is given by

$$r_i = x_i^{l_i-1} [x_i^{-1}, y_i^{-1}], \quad i = 1, \dots, n$$

and we have

$$r_i \equiv x_i^{l_i-1} \prod_{\substack{0 \leq j \leq n \\ j \neq i}} [x_i, x_j]^{a'_{i,j}} \pmod{F_{(3)}}$$

where the numbers  $a'_{i,j} \in \mathbb{F}_2$  are given by

$$a'_{i,j} = \begin{cases} a_{i,j} + \tilde{a}_{i,0}, & \text{if } l_j \equiv 3 \pmod{4}, \\ a_{i,j}, & \text{else.} \end{cases}$$

*Proof.* This is a special case of [3], Th.11.10. In fact, first note that since  $2 \in S$ , we have  $\text{III}_S(2) = \text{B}_S(2) = 0$ . By class field theory and 3.1 it follows that the set  $\{\tau_0, \tau_1, \dots, \tau_n\}$  is a minimal system of generators of  $G_S(2)$ . A system of defining relations is given by the local relations

$$\begin{aligned} r_0 &= \tilde{x}_0^2 [x_0, y_0] r'_0, \\ r_i &= x_i^{l_i-1} [x_i^{-1}, y_i^{-1}], \quad i = 1, \dots, n \end{aligned}$$

for some  $r'_0 \in F_{(2)}$  where  $\tilde{x}_0$  denotes a preimage of  $\tilde{\tau}_0$  under  $\pi$ , cf. 3.2. Any of these relations may be omitted and we decide to ignore  $r_0$ . According to the choices we have made and by definition of the linking numbers  $a_{i,j}$  the elements  $y_i$  satisfy

$$y_i \equiv x_0^{a_{i,0}} \tilde{x}_0^{\tilde{a}_{i,0}} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} x_j^{a_{i,j}} \pmod{F_{(2)}}.$$

Class field theory implies

$$\tilde{x}_0 \equiv \prod_{\substack{1 \leq j \leq n, \\ l_j \equiv 3 \pmod{4}}} x_j \pmod{F_{(2)}}$$

which finishes the proof.  $\square$

**Corollary 3.5.** *Let the set  $S$  be given as in 3.4. For the Zassenhaus invariant of  $G_S(2)$  we have  $\mathfrak{z}(G_S(2)) \geq 3$  if and only if  $l_i \equiv 1 \pmod{8}$ ,  $i = 1, \dots, n$  and the Legendre symbols satisfy*

$$\left(\frac{l_i}{l_j}\right)_2 = 1, \quad 1 \leq i, j \leq n, \quad i \neq j.$$

*Proof.* Keeping the notation of 3.4, the cup-product vanishes if and only if  $R \subseteq F_{(3)}$ , i.e.  $r_i \in F_{(3)}$  for  $1 \leq i \leq n$ . The latter is equivalent to  $x_i^{l_i-1} \in F_{(3)}$  and  $a'_{i,j} = 0$  for  $1 \leq i \leq n$ ,  $0 \leq j \leq n$ ,  $i \neq j$ . Noting that for  $1 \leq i \leq n$  we have  $x_i^{l_i-1} \in F_{(3)}$  if and only if  $l_i \equiv 1 \pmod{4}$ , the claim follows immediately from the definition of the numbers  $a'_{i,j}$ .  $\square$

#### 4. RÉDEI SYMBOLS

We fix a set

$$S = \{2, l_1, \dots, l_n\}$$

where  $l_i \equiv 1 \pmod{8}$ ,  $i = 1, \dots, n$  are pairwise distinct prime numbers with Legendre symbols  $\left(\frac{l_i}{l_j}\right) = 1$ ,  $1 \leq i, j \leq n$ ,  $i \neq j$ .

By 3.5, there exists a uniquely defined triple Massey product

$$H^1(G_S(2)) \times H^1(G_S(2)) \times H^1(G_S(2)) \longrightarrow H^2(G_S(2))$$

determining the relation structure of  $G_S(2)$  modulo the fourth step of the Zassenhaus filtration. Under some further conditions on the primes in  $S$ , we will give an explicit description of this product in terms of certain arithmetical symbols called *Rédei symbols*. These symbols have first been introduced in [10] in order to study diophantine equations.

For the definition of the Rédei symbol  $[\cdot, \cdot, \cdot]$ , we need the following notation:

**Definition 4.1.** Let  $k$  be a number field,  $\alpha \in k^\times \setminus k^{\times 2}$  and let  $\mathfrak{p}$  be a prime ideal of  $k$ . Then we set

$$\left(\frac{\alpha|k}{\mathfrak{p}}\right) = \begin{cases} 1, & \text{if } \mathfrak{p} \text{ splits in } k(\sqrt{\alpha}), \\ 0, & \text{if } \mathfrak{p} \text{ is ramified in } k(\sqrt{\alpha}), \\ -1, & \text{if } \mathfrak{p} \text{ is inert in } k(\sqrt{\alpha}). \end{cases}$$

**Proposition 4.2.** *Let  $0 \leq i, j \leq n$  such that  $(i, j) \neq (0, 0)$ . Let  $k_1$  denote the real quadratic number field  $k_1 = \mathbb{Q}(\sqrt{l_i})$ . Then there exists an element  $\alpha \in k_1$  satisfying the following properties:*

- (1)  $N_{k_1|\mathbb{Q}}(\alpha) = l_j z^2$  for some  $z \in \mathbb{Z}$  where  $N_{k_1|\mathbb{Q}}(\cdot)$  denotes the norm,
- (2)  $N_{k_1|\mathbb{Q}}(D_{k_{12}|k_1}) = l_j$  if  $j \neq 0$  or  $N_{k_1|\mathbb{Q}}(D_{k_{12}|k_1}) = 8$  if  $j = 0$  where  $k_{12} = k_1(\sqrt{\alpha})$  and  $D_{k_{12}|k_1}$  denotes the discriminant of the extension  $k_{12}|k_1$ .

In addition, let  $0 \leq k \leq n$  such that  $(l_i, l_j, l_k) = 1$ . Then there exists a prime ideal  $\mathfrak{p}$  in  $k_1$  above  $l_k$  which is unramified in  $k_{12}$ . For all such choices of  $\alpha$  and  $\mathfrak{p}$ , the symbol  $\left(\frac{\alpha|k_1}{\mathfrak{p}}\right)$  yields the same (non-zero) value.

*Proof.* This is a special case of [10], Satz 1. In fact, first suppose  $j \neq 0$ . Using the assumptions we made for the primes  $l_i$ , the classical Hasse-Minkowski theorem implies the existence of integers  $x, y, z \in \mathbb{Z}$  satisfying the equation

$$x^2 - l_i y^2 - l_j z^2 = 0,$$

such that  $(x, y, z) = 1$ ,  $x + y\sqrt{l_i} \equiv 1 \pmod{4\mathcal{O}_{k_1}}$  where  $\mathcal{O}_{k_1}$  denotes the ring of integers of  $k_1 = \mathbb{Q}(\sqrt{l_i})$ . Then  $\alpha = x + y\sqrt{l_i} \in k_1$  satisfies the conditions (1) and (2) (whereas the first condition is obvious, the second one requires a thorough examination of the discriminant for which we refer the reader to [10]). Now assume that  $i \neq 0$  and  $\alpha' \in k_2 = \mathbb{Q}(\sqrt{l_j})$  satisfies conditions (1) and (2) after replacing  $l_j$  by  $l_i$ . Then again by [10] the element

$$\alpha = \text{Tr}_{k_2|\mathbb{Q}}(\alpha') + 2\sqrt{N_{k_2|\mathbb{Q}}(\alpha')} = (\sqrt{\alpha'} + \sqrt{\alpha'})^2 \in k_1$$

satisfies conditions (1) and (2). For the second part of the proposition we again refer to [10], Satz 1.  $\square$

**Definition 4.3.** Let  $0 \leq i, j, k \leq n$  such that  $(i, j) \neq (0, 0)$ . Keeping the notations and assumptions of 4.2, the Rédei symbol  $[l_i, l_j, l_k] \in \{\pm 1\}$  is defined by

$$[l_i, l_j, l_k] = \left(\frac{\alpha|k_1}{\mathfrak{p}}\right).$$

Furthermore, we set

$$[l_0, l_0, l_k] = \begin{cases} 1, & \text{if } l_k \equiv 1 \pmod{16}, \\ -1, & \text{if } l_k \equiv 9 \pmod{16}. \end{cases}$$

If  $(i, j) \neq (0, 0)$ , by definition the Rédei symbol  $[l_i, l_j, l_k]$  describes the decomposition behavior of the prime  $l_k$  in the field  $\mathbb{Q}(\sqrt{l_i})(\sqrt{\alpha})$ . If  $i = j = 0$ , it describes the decomposition behavior of  $l_k$  in the maximal real subfield of the cyclotomic field  $\mathbb{Q}(\zeta_{16})$ . In the original paper [10], Rédei proves the remarkable fact that the symbol  $[\cdot, \cdot, \cdot]$  is symmetric: For any permutation  $\gamma$  of the indices  $\{i, j, k\}$  it holds that

$$[l_i, l_j, l_k] = [l_{\gamma(i)}, l_{\gamma(j)}, l_{\gamma(k)}].$$

Let  $K_{i,j}$  denote the Galois closure of  $\mathbb{Q}(\sqrt{l_i})(\sqrt{\alpha})|\mathbb{Q}$ . It is also the Galois closure of the field  $\mathbb{Q}(\sqrt{l_j})(\sqrt{\alpha'})$  where  $\alpha'$  is given as in 4.2 after exchanging  $l_i$  and  $l_j$ . Furthermore,  $\mathbb{Q}(\sqrt{l_i}, \sqrt{l_j}) \subseteq K_{i,j}$ . For the structure of the Galois group  $G(K_{i,j}|\mathbb{Q})$  we have the following result proven in [10]:

**Proposition 4.4.** *Keeping the notations and assumptions of 4.2, the following holds for  $(i, j) \neq (0, 0)$ :*

- (i) *If  $l_i \neq l_j$ , then  $G(K_{i,j}|\mathbb{Q})$  is the dihedral group of order 8. Let  $s, t$  be generators of  $G(K_{i,j}|\mathbb{Q}(\sqrt{l_i})(\sqrt{\alpha}))$  and  $G(K_{i,j}|\mathbb{Q}(\sqrt{l_i})(\sqrt{\alpha'}))$  respectively, i.e.*

$$s : \sqrt{\alpha} \mapsto -\sqrt{\alpha}, \quad t : \sqrt{\alpha'} \mapsto -\sqrt{\alpha'}$$

where  $\alpha'$  is given as in 4.2 after exchanging  $l_i$  and  $l_j$ . Then  $G(K_{i,j}|\mathbb{Q})$  admits the presentation

$$G(K_{i,j}|\mathbb{Q}) = \langle s, t \mid s^2 = t^2 = (st)^4 = 1 \rangle.$$

If  $l_i = l_j$ , then  $K_{i,j}$  is a cyclic extension of degree 4 over  $\mathbb{Q}$ .

(ii) The discriminant of  $K_{a_1, a_2}$  is given by

$$D_{K_{i,j}|\mathbb{Q}} = \begin{cases} \overline{l_i}^4 \overline{l_j}^4, & \text{if } l_i \neq l_j, \\ l_i^3, & \text{if } l_i = l_j \end{cases}$$

where we have set  $\overline{l_i} = l_i$  for  $i \neq 0$  and  $\overline{l_0} = 8$ . In particular,  $K_{i,j}|\mathbb{Q}$  is unramified outside the set  $\{l_i, l_j, \infty\}$ .

**Definition 4.5.** Keeping the notation of 4.2, we say that the pair  $(l_i, l_j)$  is *totally real* if  $i = j = 0$  or the element  $\alpha$  can be chosen in such a way that  $\mathbb{Q}(\sqrt{l_i})(\sqrt{\alpha})$  and hence  $K_{i,j}$  is totally real.

By 4.4, we have  $K_{i,j} \subseteq \mathbb{Q}_S(2)$  if and only if  $(l_i, l_j)$  is totally real. We are thus led to the question for sufficient and necessary conditions for this property. First observe that  $\mathbb{Q}(\sqrt{l_i})(\sqrt{\alpha})$  is totally real if and only if the Diophantine equation  $x^2 - l_i y^2 - l_j z^2 = 0$  in the proof of 4.2 admits a solution  $(x, y, z)$  with  $x > 0$ . We have the following

**Proposition 4.6.**

- (i) For  $1 \leq i \leq n$ , the pair  $(l_i, l_i)$  is totally real.
- (ii) For  $1 \leq i \leq j \leq n$ ,  $i \neq j$  the field  $K_{i,j}$  is the unique Galois extension of degree 4 of the quadratic field  $\mathbb{Q}(\sqrt{l_i l_j})$  unramified outside the infinite primes. In particular, it is independent of the choice of the element  $\alpha$  in 4.2.
- (iii) For  $1 \leq i \leq j \leq n$ ,  $i \neq j$  the following assertions are equivalent:
  - (1) The pair  $(l_i, l_j)$  is totally real.
  - (2) The class number of  $\mathbb{Q}(\sqrt{l_i l_j})$  is divisible by 4.
  - (3) The class number of  $\mathbb{Q}(\sqrt{l_i}, \sqrt{l_j})$  is even.
  - (4) For the fourth power residue symbol  $(\cdot)_4$  it holds that

$$\left(\frac{l_i}{l_j}\right)_4 = \left(\frac{l_j}{l_i}\right)_4.$$

*Proof.* In order to show (i), note that  $l_i$  can be written as  $l_i = y^2 + z^2$  with  $y \equiv 0 \pmod{4}$ . This gives rise to a solution of the equation  $x^2 - l_i y^2 - l_j z^2$  satisfying the properties in the proof of 4.2 with  $x = l_i > 0$  which shows (i).

For  $i \neq j$ , a straightforward examination of the subfields of  $K_{i,j}$  shows that  $K_{i,j}|\mathbb{Q}(\sqrt{l_i l_j})$  is a cyclic extension of degree 4 unramified at all finite places, cf. [10]. By Gauss' genus theory, the 2-rank of the narrow class group of  $\mathbb{Q}(\sqrt{l_i l_j})$  is 1 (e.g. see [4]) showing (ii).

If  $(l_i, l_j)$  is totally real,  $K_{i,j}|\mathbb{Q}(\sqrt{l_i l_j})$  is an unramified extension of degree 4 implying (2). Conversely, assuming (2), the field  $\mathbb{Q}(\sqrt{l_i l_j})$  possesses an unramified extension of degree 4 which by (ii) must coincide with  $K_{i,j}$ . Hence (1) holds. For the equivalences  $(2) \Leftrightarrow (3) \Leftrightarrow (4)$  see [6], Th.1.  $\square$

We can now state and prove the fundamental relation between the triple Massey products for the group  $G_S(2)$  and Rédei symbols. We keep the system of generators  $\tau_i$  and relations  $r_i$  as chosen in 3.4.

**Theorem 4.7.** *Let  $S = \{l_0, \dots, l_n\}$  where  $l_0 = 2$  and  $l_1, \dots, l_n$  are prime numbers  $\equiv 1 \pmod{8}$  satisfying  $\left(\frac{l_i}{l_j}\right)_2 = 1$ ,  $1 \leq i, j \leq n$ ,  $i \neq j$ . Then the group  $G_S(2)$  has Zassenhaus invariant  $\mathfrak{z}(G_S(2)) \geq 3$  and the triple Massey product*

$$\langle \cdot, \cdot, \cdot \rangle_n : H^1(G_S(2)) \times H^1(G_S(2)) \times H^1(G_S(2)) \longrightarrow H^2(G_S(2))$$

*is given by*

$$(-1)^{\text{tr}_{r_m} \langle \chi_i, \chi_j, \chi_k \rangle_3} = \begin{cases} [l_i, l_j, l_k], & \text{if } m = k, m \neq i, \\ [l_j, l_k, l_i], & \text{if } m = i, m \neq k, \\ 1, & \text{otherwise} \end{cases}$$

*for all  $1 \leq m \leq n$  and provided that  $(l_i, l_j)$  and  $(l_j, l_k)$  are totally real. Here  $\chi_0, \dots, \chi_n \in H^1(G_S(2))$  denotes the basis dual to the system of generators  $\tau_0, \dots, \tau_n$  of  $G_S(2)$  chosen as in 3.4 and  $\text{tr}_{r_m} : H^2(G_S(2)) \rightarrow \mathbb{F}_2$  is the trace map corresponding to the relation  $r_m$ .*

*Proof.* First assume that  $i \neq j$ . We set  $k_1 = \mathbb{Q}(\sqrt{l_i})$ ,  $k_2 = \mathbb{Q}(\sqrt{l_j})$ . By 4.2, it follows that there exists a prime  $\mathfrak{p}_j$  in  $k_1$  over  $l_j$  which is unramified in  $k_1(\sqrt{\alpha})$ . We have the presentation

$$G(K_{i,j}|\mathbb{Q}) = \langle s, t \mid s^2 = t^2 = (st)^4 = 1 \rangle$$

where  $s, t$  are chosen as in 4.4(i). Since by 4.4(ii)  $l_j$  ramifies in  $K_{i,j}$ , it follows that there is a prime  $\mathfrak{P}_j$  in  $K_{i,j}$  above  $l_j$  such that the inertia group  $T_{\mathfrak{P}_j}$  is generated by  $s$ . It follows from symmetry that there exists a prime  $\mathfrak{P}_i$  in  $K_{i,j}$  above  $l_i$  such that the inertia group  $T_{\mathfrak{P}_i}$  is generated by  $t$ . Assuming that the pair  $(l_i, l_j)$  is totally real, we have  $K_{i,j} \subseteq \mathbb{Q}_S(2)$  and we may choose primes  $\mathfrak{l}_i, \mathfrak{l}_j$  in  $\mathbb{Q}_S(2)$  lying above  $\mathfrak{P}_i, \mathfrak{P}_j$ . For all  $0 \leq k \leq n$ ,  $k \neq i, j$ , we choose an arbitrary prime in  $\mathbb{Q}_S(2)$  above  $l_k$ .

As in 3.4 we have a minimal presentation  $1 \rightarrow R \rightarrow F \rightarrow G_S(2) \rightarrow 1$  where  $F$  is the free pro-2-group on  $x_0, \dots, x_n$  and  $x_k$  maps to  $\tau_k \in T_{\mathfrak{l}_k}$  for all  $0 \leq k \leq n$  and hence we have a projection

$$\pi : F \twoheadrightarrow G_S(2) \twoheadrightarrow G(K_{i,j}|\mathbb{Q}).$$

Since by 4.4  $K_{l_i, l_j}$  is unramified outside  $\{l_i, l_j\}$ , we have  $\pi(x_k) = 1$ ,  $k \neq i, j$ . Furthermore,  $\pi(x_i) = t$ , since  $\pi(x_i)$  is contained in  $T_{\mathfrak{P}_i}$  and must be non-trivial. In fact, if  $1 \leq i \leq n$ , this follows immediately from the observation that  $\tau_i$  is a generator of the inertia subgroup  $T_{\mathfrak{l}_i} \subseteq G_S(2)$  of  $\mathfrak{l}_i$ . For  $i = 0$  we can argue as follows: Suppose  $\pi(x_0) = 1$ , then the restriction of  $\tau_0$  to  $k_1 = \mathbb{Q}(\sqrt{2})$  is trivial. On the other hand, the restriction of  $\tau_0$  to  $\mathbb{Q}_S(2)^{ab}$  equals  $(\hat{g}_0, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$  where

$\hat{g}_0$  denotes the idèle whose 2-component is 5 and whose other components are 1. Since  $(\hat{g}_0, \mathbb{Q}(\sqrt{2})|\mathbb{Q})$  is the non-trivial element in  $\text{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$ , this yields a contradiction. By symmetry, we conclude that

$$\pi(x_k) = \begin{cases} t, & \text{if } k = i, \\ s, & \text{if } k = j, \\ 1, & \text{if } k \neq i, j. \end{cases}$$

Now let  $k \in \{1, \dots, n\}$  such that  $k \neq i, j$  and let  $\mathfrak{p}_k$  denote a prime ideal in  $k_1$  above  $l_k$  unramified in  $k_1(\sqrt{\alpha})$ . Choose a prime  $\mathfrak{P}_k$  in  $k_1 k_2 = \mathbb{Q}(\sqrt{l_i}, \sqrt{l_j})$  above  $\mathfrak{p}_k$ . By our assumptions on the Legendre symbols,  $l_k$  is completely decomposed in  $k_1 k_2$  and hence  $\mathfrak{p}_k$  splits in  $k_1(\sqrt{\alpha})$  if and only if  $\mathfrak{P}_k$  splits in  $k_1 k_2(\sqrt{\alpha}) = K_{i,j}$ , i.e. we have

$$\left( \frac{\alpha|k_1}{\mathfrak{p}_k} \right) = \left( \frac{\alpha|k_1 k_2}{\mathfrak{P}_k} \right).$$

Noting that  $G(K_{l_i, l_j} | k_1 k_2)$  is generated by  $(st)^2$  and since by definition the element  $y_k \in F$  (chosen with respect to a prolongation  $\mathfrak{l}_k$  of  $\mathfrak{P}_k$  to  $\mathbb{Q}_S(2)$ ) is mapped via  $\pi$  to the Frobenius of the prime lying under  $\mathfrak{l}_k$  in  $K_{i,j}$ , it follows that

$$\pi(y_k) = \begin{cases} (st)^2, & \text{if } [l_i, l_j, l_k] = -1, \\ 1, & \text{if } [l_i, l_j, l_k] = 1. \end{cases}$$

By 4.4(i) the kernel  $\tilde{R}$  of  $\pi : F \rightarrow G(K_{\tilde{l}_i, \tilde{l}_j} | \mathbb{Q})$  is generated by the elements  $x_i^2, x_j^2, (x_j x_i)^4$  and  $x_l$ ,  $l \neq i, j$  as closed normal subgroup of  $F$ . A straightforward computation of the Magnus expansions (cf. 2.3) of these elements yields

$$\begin{aligned} \psi(x_i^2) &= 1 + X_i^2, \\ \psi(x_j^2) &= 1 + X_j^2, \\ \psi((x_j x_i)^4) &\equiv 1 \pmod{\deg \geq 4} \\ \psi(x_l) &= 1 + X_l. \end{aligned}$$

Therefore the maps  $\varepsilon_{(i),2}, \varepsilon_{(j),2}, \varepsilon_{(i,j),2}$  vanish identically on  $\tilde{R}$ . If  $[\tilde{l}_i, \tilde{l}_j, l_k] = 1$ , we have  $y \in \tilde{R}$  and consequently  $\varepsilon_{(i,j),2}(y_k) = 0$ . If  $[\tilde{l}_i, \tilde{l}_j, l_k] = -1$ , then  $\pi(y_k) = (st)^2$ , i.e.  $y_k = (x_j x_i)^2 r$  for some  $r \in \tilde{R}$ . This yields

$$\varepsilon_{(i,j),2}(y_k) = \varepsilon_{(i,j),2}((x_i x_j)^2) + \varepsilon_{(i,j),2}(r) + \varepsilon_{(i),2}((x_i x_j)^2) \varepsilon_{(j),2}(r) = 1$$

where we have used the product formula [12], Prop.1.1.22.

Next we consider the case  $k = j$ , so in particular  $j \neq 0$ . By definition of the Rédei symbol, if  $[l_i, l_j, l_j] = 1$ , we have the decomposition

$$l_j \mathcal{O}_{k_1(\sqrt{\alpha_2})} = \mathfrak{q}_1 \mathfrak{q}_2 \mathfrak{q}_3^2$$

with pairwise different prime ideals  $\mathfrak{q}_i$ . By choice of the prime  $\mathfrak{P}_j$  of  $K_{i,j}$ , we have  $\mathfrak{P}_j \mid \mathfrak{q}_1$  or  $\mathfrak{P}_j \mid \mathfrak{q}_2$ . The Frobenius automorphism of  $\mathfrak{l}_j$  maps to the trivial element of  $\text{Gal}(k_1(\sqrt{\alpha_2})|\mathbb{Q})$ , i.e.  $\pi(y_j) = 1$  or  $\pi(y_j) = s$ . We recall that the restriction of the image  $\sigma_j$  of  $y_j$  in  $G_S(2)$  to  $\mathbb{Q}_S(2)^{ab}$  is given by  $(\hat{l}_j, \mathbb{Q}_S(2)^{ab}|\mathbb{Q})$  where  $\hat{l}_j$  denotes the idèle whose  $l_j$ -component equals  $l_j$  and all other components are 1, i.e. by class field theory the restriction of  $\sigma_j$  to  $k_2 =$

$\mathbb{Q}(\sqrt{l_j})$  is trivial. Since  $s$  maps  $\sqrt{l_j}$  to  $-\sqrt{l_j}$ , the case  $\pi(y_j) = s$  cannot occur and in particular  $\varepsilon_{(i,j),2}(y_k) = 0$  holds. If  $[l_i, l_j, l_j] = -1$ , then  $l_j$  decomposes as

$$l_j \mathcal{O}_{k_1(\sqrt{\alpha_2})} = \mathfrak{q}_1 \mathfrak{q}_2^3$$

where  $\mathfrak{P}_j \mid \mathfrak{q}_1$ . In this case the Frobenius automorphism of  $\mathfrak{l}_j$  maps to the non-trivial automorphism of  $k_1(\sqrt{\alpha_2})|k_1$  and we have  $\pi(y_j) = (st)^2$  or  $\pi(y_j) = s(st)^2$  where again the latter case cannot occur, since  $s(st)^2$  maps  $\sqrt{l_j}$  to  $-\sqrt{l_j}$ . As in the case  $k \neq j$  we conclude that  $\varepsilon_{(i,j),2}(y_j) = 1$ . By symmetry,  $\varepsilon_{(i,j),2} = 1$  if and only if  $[l_i, l_j, l_i] = -1$ .

In order to determine  $\varepsilon_{(i,i),2}(y_k)$  for  $1 \leq i, k \leq n$ ,  $i \neq j$ , first note that by 4.4  $K_{i,i}|\mathbb{Q}$  is a cyclic extension of degree 4 and that by 4.6(i)  $K_{l_i, l_i} \subseteq \mathbb{Q}_S(2)$ . More precisely,  $K_{i,i}$  is unramified outside  $l_i$  and totally ramified at  $l_i$ . We can choose a minimal presentation  $1 \rightarrow R \rightarrow F \rightarrow G_S(2) \rightarrow 1$ , such that the induced projection  $\pi : F \rightarrow G(K_{l_i, l_i}|\mathbb{Q})$  maps  $x_l$  to 1 for  $l \neq i$  and  $x_i$  to  $s$  where  $s$  is a generator of  $G(K_{i,i}|\mathbb{Q})$ . By definition it holds that

$$\pi(y_k) = \begin{cases} s^2, & \text{if } [l_i, l_i, l_k] = -1, \\ 1, & \text{if } [l_i, l_i, l_k] = 1. \end{cases}$$

Again let  $\tilde{R}$  be the kernel of  $\pi : F \twoheadrightarrow G(K_{\tilde{l}_i, \tilde{l}_j}|\mathbb{Q})$ , i.e.  $\tilde{R}$  is the closed normal subgroup of  $F$  generated by  $x_i^4, x_l, k \neq i$ . Since

$$\psi(x_i^4) = 1 + X_i^4,$$

we see that in particular  $\varepsilon_{(i,i),2}, \varepsilon_{i,2}$  vanish on  $\tilde{R}$ . Hence if  $\pi(y_k) = 1$ , we have  $\varepsilon_{(i,i),2}(y_k) = 0$ . If  $\pi(y_k) = s^2$ , then  $y_k = x_i^2 r$  for some  $r \in \tilde{R}$  which implies that

$$\varepsilon_{(i,i),2}(y_k) = \varepsilon_{(i,i),2}(x_i^2) + \varepsilon_{(i,i),2}(r) + \varepsilon_{(i),2}(x_i^2)\varepsilon_{(i),2}(r) = 1.$$

Since  $\pi(y_i) = 1$ , by the same argument we obtain  $\mu_2(i, i, i) = 0$ , showing the first part of (ii).

Finally we consider the case  $(i, j) = (0, 0)$ . Let  $K = \mathbb{Q}(\zeta_{16})^+$  denote the maximal real subfield of the cyclotomic field  $\mathbb{Q}(\zeta_{16})$ . The extension  $K|\mathbb{Q}$  is cyclic of degree 4 over  $\mathbb{Q}$  and  $K \subseteq \mathbb{Q}_S(2)$ . Let  $s \in G(K|\mathbb{Q})$  denote a generator. By definition of the symbol  $[l_0, l_0, l_k]$ , we have a projection

$$\pi : F \twoheadrightarrow G_S(2) \twoheadrightarrow G(K|\mathbb{Q})$$

such that for all  $1 \leq k \leq n$

$$\pi(y_k) = \begin{cases} s^2, & \text{if } [l_0, l_0, l_k] = -1, \\ 1, & \text{if } [l_0, l_0, l_k] = 1. \end{cases}$$

Hence as in the case  $i = j, i \neq 0$  we conclude that  $\varepsilon_{(0,0),2}(y_j) = 1$  if and only if  $[l_0, l_0, l_j] = -1$ .

Summing up, for  $(i, j, k), 0 \leq i, j \leq n, 1 \leq k \leq n$  we have the identities

$$\varepsilon_{(i,j),2}(y_k) = \begin{cases} 1, & \text{if } [l_i, l_j, l_k] = -1, \\ 0, & \text{if } [l_i, l_j, l_k] = 1. \end{cases}$$



Hence for  $1 \leq m \leq n$  it follows from 2.4 that

$$\begin{aligned}
 tr_{r_m} \langle \chi_i, \chi_j, \chi_k \rangle_3 &= \varepsilon_{(i,j,k),2}(r_m) = \varepsilon_{(i,j,k),2}(x_m^{l_m-1} [x_m^{-1}, y_m^{-1}]) \\
 &= \varepsilon_{(i,j,k),2}([x_m^{-1}, y_m^{-1}]) \\
 &= \varepsilon_{(i),2}(x_m^{-1}) \varepsilon_{(j,k),2}(y_m^{-1}) - \varepsilon_{(k),2}(x_m^{-1}) \varepsilon_{(i,j),2}(y_m^{-1}) \\
 &= \begin{cases} 1, & \text{if } m = k, m \neq i, [l_i, l_j, l_k] = -1, \\ 1, & \text{if } m = i, m \neq k, [l_i, l_j, l_k] = -1, \\ 0, & \text{otherwise} \end{cases}
 \end{aligned}$$

where we have used the identities for the maps  $\varepsilon_{\cdot,2}$  given in [13], Prop.1.1.22. This concludes the proof.  $\square$

**Remark 4.8.** For triple Massey products of the form  $\langle \chi_i, \chi_j, \chi_k \rangle_3$ ,  $i, j, k \neq 0$ , the above proof follows the ideas given in [12] and [8]. The main difficulty comes from the fact that  $2 \in S$  in our case which amounts to calculating Massey products for  $\chi_0$ .

Together with Theorem 2.8 this enables us to prove the main result of this section which gives a large supply of mild pro-2-groups of the form  $G_S(2)$  with Zassenhaus invariant 3:

**Theorem 4.9.** *Let  $S = \{l_0, l_1, \dots, l_n\}$  for some  $n \geq 1$  and prime numbers  $l_0 = 2$ ,  $l_i \equiv 9 \pmod{16}$ ,  $i = 1, \dots, n$ , such that the Legendre symbols satisfy*

$$\left( \frac{l_i}{l_j} \right)_2 = 1, \quad 1 \leq i, j \leq n, \quad i \neq j.$$

*Then  $G_S(2)$  is a mild pro-2-group with generator rank  $n + 1$ , relation rank  $n$  and Zassenhaus invariant  $\mathfrak{z}(G) = 3$ .*

*Proof.* We have already seen that  $\mathfrak{z}(G_S(2)) \geq 3$ . As in 4.7 let  $\chi_0, \dots, \chi_n \in H^1(G_S(2))$  denote the dual basis of the system of generators  $\tau_0, \dots, \tau_n$ . Since by assumption  $l_1 \equiv \dots \equiv l_n \equiv 9 \pmod{16}$ , by 4.7 we obtain

$$tr_{r_m} \langle \chi_0, \chi_0, \chi_k \rangle_3 = tr_{r_m} \langle \chi_k, \chi_0, \chi_0 \rangle_3 = \delta_{mk} = \begin{cases} 1, & \text{if } m = k, \\ 0, & \text{if } m \neq k \end{cases}$$

for  $m = 1, \dots, n$ . Note that we have used the shuffle identity [2], Prop.4.8. In particular, the triple Massey product is non-zero and therefore  $\mathfrak{z}(G_S(2)) = 3$ . We apply 2.8 with respect to the subspaces  $U, V$  spanned by  $\{\chi_1, \dots, \chi_n\}$  and  $\{\chi_0\}$  respectively and  $e = 1$ . Noting that  $tr_{r_1}, \dots, tr_{r_n}$  is a basis of  $H^2(G_S(2))^\vee$ , the above observation implies that the  $\mathbb{F}_2$ -linear map  $U \otimes V \otimes V \rightarrow H^2(G_S(2))$  is an isomorphism, i.e. condition (b) of 2.8 is satisfied. Furthermore, again by [2], Prop.4.8 we have  $\langle \chi_0, \chi_0, \chi_0 \rangle_3 = 0$ . Hence, condition (a) also holds and we conclude that  $G_S(2)$  is mild with respect to the Zassenhaus filtration.  $\square$

In the above proof we only had to calculate Massey products of the form  $\langle \chi_0, \chi_0, \chi_k \rangle_3$ . In the following examples all pairs of primes  $(l_i, l_j)$  are totally real, so we get an entire description of the triple Massey product:

**Example 4.10.**

(i) Let  $S = \{l_0, \dots, l_4\}$  where

$$l_0 = 2, \quad l_1 = 313, \quad l_2 = 457, \quad l_3 = 521.$$

We have  $\left(\frac{313}{457}\right)_2 = \left(\frac{313}{521}\right)_2 = \left(\frac{457}{521}\right)_2 = 1$  and a calculation of solutions of the diophantine equation in the proof of 4.2 shows that all pairs  $(l_i, l_j)$  are totally real. Using the computational algebra system MAGMA [1], we find that the symbol  $[l_i, l_j, l_k]$  is  $-1$  for all permutations of the triples

$$(i, j, k) = (1, 1, 3), (1, 2, 3), (1, 3, 3), (0, 0, 1), (0, 0, 2), (0, 0, 3), \\ (0, 1, 1), (0, 2, 2), (0, 3, 3), (0, 2, 3), (0, 3, 2)$$

and  $[l_i, l_j, l_k] = 1$  in all other cases. By 4.9,  $G_S(2)$  is mild.

(ii) Let  $S = \{l_0, l_1, l_2\}$  where

$$l_0 = 2, \quad l_1 = 113, \quad l_2 = 593.$$

Computations using MAGMA [1] show that all pairs of primes in  $S$  are totally real and that all Rédei symbols are equal to 1. Hence, the triple Massey product of  $G_S(2)$  is identically zero, i.e. we have  $\mathfrak{z}(G_S(2)) \geq 4$ .

## 5. FABULOUS PRO-2-GROUPS WITH TRIVIAL CUP-PRODUCT

Let  $k$  be a number field and  $S$  be a finite set of primes of  $k$  disjoint from the places  $S_p$  lying above  $p$ . Then the maximal pro- $p$ -extension  $k_S(p)|k$  unramified outside  $S$  does not contain any  $\mathbb{Z}_p$ -extension and therefore its Galois group  $G_S(p)$  has finite abelianization. More precisely,  $G_S(p)$  is a fab pro- $p$ -group:

**Definition 5.1.** A pro- $p$ -group  $G$  is called *fab* if for every open subgroup  $H \subseteq G$  the abelianization  $H^{ab} = H/[H, H]$  is finite. We call  $G$  *fabulous* if it is mild and fab.

If a fab pro- $p$ -group  $G$  is of cohomological dimension 2, it is a duality group of strict cohomological dimension 3. In particular, this holds for any fabulous group. The first examples of fabulous groups of the form  $G_S(p)$  have been constructed by J. Labute [7] over  $k = \mathbb{Q}$ . The results of A. Schmidt et. al. provide an infinite supply of examples over arbitrary number fields. One should also remark the relevance of arithmetical fab groups with regard to the Fontaine-Mazur conjecture.

However, from a group theoretical point of view, fabulous pro- $p$ -groups are not yet well understood. To the author's knowledge, to date there is no known example of a non-analytic fab pro- $p$ -group being explicitly described in terms of generators and relations. Therefore, it seems desirable to obtain examples of fabulous pro- $p$ -groups with a more explicit knowledge of the relation structure, e.g. by a complete determination of the triple Massey product.

The groups  $G_S(2)$  studied in the previous section are not fab since we had to allow wild ramification, i.e.  $2 \in S$ . It turns out that one can produce fab (and even fabulous) quotients of these groups by adding further arithmetic conditions:

If  $k$  is a number field and  $S, T$  are disjoint finite sets of primes of  $k$ , we denote by  $G_S^T(p)$  the Galois group of the maximal  $p$ -extension  $k_S^T(p)$  of  $k$  which is unramified outside  $S$  and completely decomposed at the primes above  $T$ .

For  $k = \mathbb{Q}$ ,  $p = 2$ ,  $\#T = 1$  we obtain the following

**Theorem 5.2.** *Let  $S = \{l_0, \dots, l_n\}$  where  $l_0 = 2$  and  $l_1, \dots, l_n$  are prime numbers  $\equiv 1 \pmod{8}$  satisfying  $\left(\frac{l_i}{l_j}\right)_2 = 1$ ,  $1 \leq i, j \leq n$ ,  $i \neq j$ . Furthermore, let  $T = \{q\}$  where  $q \notin S$  is a prime number  $\equiv 5 \pmod{8}$ , such that the following conditions are satisfied:*

- (1)  $\left(\frac{q}{l_i}\right) = 1$  for all  $i = 1, \dots, n-1$ ,
- (2)  $\left(\frac{q}{l_n}\right) = -1$ .

Then for the pro-2-group  $G_S^T(2)$  the following holds:

- (i)  $G_S^T(2)$  has generator rank  $h^1(G_S^T(2)) = n$ , relation rank  $h^2(G_S^T(2)) \leq n$  and Zassenhaus invariant  $\mathfrak{z}(G_S^T(2)) \geq 3$ .
- (ii) Assume that the pair  $(l_i, l_j)$  is totally real for all  $0 \leq i, j \leq n$ ,  $i \neq j$ . Then  $G_S^T(2)$  possesses a presentation  $G_S^T(2) = \langle \bar{x}_1, \dots, \bar{x}_n \mid \bar{\tau}_1, \dots, \bar{\tau}_n \rangle$  such that the triple Massey product

$$\langle \cdot, \cdot, \cdot \rangle_3 : H^1(G_S^T(2)) \times H^1(G_S^T(2)) \times H^1(G_S^T(2)) \longrightarrow H^2(G_S^T(2))$$

is given by

$$(-1)^{tr_{\bar{\tau}_m} \langle \bar{x}_i, \bar{x}_j, \bar{x}_k \rangle_3} = \begin{cases} [l_i, l_j, l_k], & \text{if } m = k, \ m \neq i, \ i, j \neq n, \\ [l_i, l_j, l_k] \cdot [l_0, l_j, l_k], & \text{if } m = k, \ i = n, j \neq n, \\ [l_i, l_j, l_k] \cdot [l_0, l_j, l_k], & \text{if } m = k, \ m \neq i, \ i \neq n = j, \\ [l_i, l_j, l_k] \cdot [l_0, l_j, l_k], & \text{if } m = k, \ i = j = n, \\ [l_j, l_k, l_i], & \text{if } m = k, \ m \neq i, i, j \neq n, \\ [l_j, l_k, l_i] \cdot [l_0, l_j, l_k], & \text{if } m = i, \ k = n, \ j \neq n, \\ [l_j, l_k, l_i] \cdot [l_0, l_k, l_i], & \text{if } m = i, \ m \neq k, \ k \neq n = j, \\ [l_j, l_k, l_i] \cdot [l_0, l_0, l_i], & \text{if } m = i, \ k = j = n, \\ 1, & \text{otherwise} \end{cases}$$

for  $m = 1, \dots, n-1$  and

$$(-1)^{tr_{\bar{\tau}_n} \langle \bar{x}_i, \bar{x}_j, \bar{x}_k \rangle_3} = \begin{cases} [l_i, l_j, l_n], & \text{if } k = n, \ i, j \neq n, \\ [l_i, l_j, l_n] \cdot [l_i, l_0, l_n], & \text{if } k = j = n, \ i \neq n, \\ [l_j, l_k, l_n], & \text{if } i = n, \ k, j \neq n, \\ [l_j, l_k, l_n] \cdot [l_0, l_k, l_n], & \text{if } i = j = n, \ k \neq n, \\ 1, & \text{otherwise} \end{cases}$$

where  $\{\bar{x}_1, \dots, \bar{x}_n\}$  denotes the basis of  $H^1(G_S^T(2))$  dual to  $\bar{x}_1, \dots, \bar{x}_n$ .

Assuming in addition that the Leopoldt conjecture holds for all number fields  $k$  contained in  $\mathbb{Q}_S^T(2)$  and the prime 2, we have:

- (iii)  $G_S^T(2)$  is a free pro-2-group and  $h^2(G_S^T(2)) = n$ .

*Proof.* Keeping the notation and choices of the elements  $\tau_0, \dots, \tau_n \in G_S(2)$  as in the previous sections, by 3.4 the group  $G_S(2)$  has a minimal presentation

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\pi} G_S(2) \longrightarrow 1$$

where  $F$  is the free pro- $p$ -group on  $x_0, \dots, x_n$ ,  $\pi$  maps  $x_i$  to  $\tau_i$  and  $R$  is generated by  $r_i = x_i^{l_i-1}[x_i^{-1}, y_i^{-1}]$ ,  $i = 1, \dots, n$  as closed normal subgroup of  $F$ . We fix a prime  $\mathfrak{Q}$  of  $\mathbb{Q}_S(2)$  lying above  $q$  and denote by  $G_{\mathfrak{Q}} \subseteq G_S(2)$  the decomposition group of  $\mathfrak{Q}$ , which is generated as closed subgroup by the Frobenius automorphism  $\sigma_{\mathfrak{Q}}$  of  $\mathfrak{Q}$ . Furthermore, we choose an arbitrary lift  $r_{\mathfrak{Q}} \in \pi^{-1}(\sigma_{\mathfrak{Q}})$ . We obtain a commutative exact diagram

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & & \downarrow & & \\
 & & & & (G_{\mathfrak{Q}}) & & \\
 & & & & \downarrow & & \\
 1 & \longrightarrow & R & \longrightarrow & F & \xrightarrow{\pi} & G_S(2) \longrightarrow 1 \\
 & & \downarrow & & \parallel & & \downarrow \\
 1 & \longrightarrow & \tilde{R} & \longrightarrow & F & \xrightarrow{\tilde{\pi}} & G_S^T(2) \longrightarrow 1 \\
 & & & & & & \downarrow \\
 & & & & & & 1
 \end{array}$$

where  $\tilde{R}$  denotes the closed normal subgroup of  $F$  generated by  $r_1, \dots, r_n, r_{\mathfrak{Q}}$  and  $(G_{\mathfrak{Q}}) \subseteq G_S(2)$  is the closed normal subgroup generated by  $G_{\mathfrak{Q}}$ . Let  $\hat{q} \in I = I_{\mathbb{Q}}$  denote the idèle of  $\mathbb{Q}$  whose  $q$ -th component equals  $q$  and all other components are 1. Then the restriction of  $\sigma_{\mathfrak{Q}}$  to  $\mathbb{Q}_S[2]$ , the maximal abelian subextension of exponent 2 in  $\mathbb{Q}_S(2)|\mathbb{Q}$ , is given by  $(\hat{q}, \mathbb{Q}_S[2]|\mathbb{Q})$  where  $(\cdot, \mathbb{Q}_S[2]|\mathbb{Q})$  denotes the global norm residue symbol. By choice of  $q$ , we have the idèlic congruence

$$\begin{aligned}
 \hat{q} &= (1, \dots, 1, q, 1, \dots) \\
 &\equiv \left(\frac{1}{q}, \dots, \frac{1}{q}, 1, \frac{1}{q}, \dots\right) \\
 &\equiv \hat{g}_0 \hat{g}_n \pmod{I_S I^2 \mathbb{Q}^\times}
 \end{aligned}$$

where

$$I_S = \prod_{l \in S} \{1\} \times \prod_{l \notin S} U_l$$

and  $\hat{g}_i$  are the idèles as constructed in the definition of the generators  $\tau_i$  of  $G_S(2)$  (cf. 3.4). Since by class field theory  $\text{Gal}(\mathbb{Q}_S[2]|\mathbb{Q}) = G_S(2)/(G_S(2))_{(2)} \cong I/I_S I^2 \mathbb{Q}^\times$ , it follows that

$$\sigma_{\mathfrak{Q}} \equiv \tau_0 \tau_n \pmod{(G_S(2))_{(2)}}, \quad r_{\mathfrak{Q}} \equiv x_0 x_n \pmod{F_{(2)}}.$$

In particular, we see that  $r_{\mathfrak{Q}} \notin F_{(2)}$  and therefore the presentation of  $G_S^T(2)$  given by the bottom horizontal line in the above diagram is *not* minimal. In order to obtain a minimal presentation, let  $\overline{F}$  be the free pro- $p$ -group on  $n$  generators  $\overline{x}_1, \dots, \overline{x}_n$ . Noting that  $r_{\mathfrak{Q}}, x_1, \dots, x_n$  is a basis of  $F$ , the mapping  $r_{\mathfrak{Q}} \mapsto 1, x_i \mapsto \overline{x}_i$ ,  $i = 1, \dots, n$  yields a well-defined surjective homomorphism  $\psi : F \longrightarrow \overline{F}$ . Let  $s$  be the section of  $\psi$  mapping  $\overline{x}_i$  to  $x_i$ ,  $i = 1, \dots, n$  and set

$\overline{R} = \psi(\tilde{R})$ . We obtain the commutative exact diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \tilde{R} & \longrightarrow & F & \xrightarrow{\tilde{\pi}} & G_S^T(2) \longrightarrow 1 \\ & & \downarrow & & \downarrow \psi & \nearrow s & \\ 1 & \longrightarrow & \overline{R} & \longrightarrow & \overline{F} & \xrightarrow{\tilde{\pi} \circ s} & G_S^T(2) \longrightarrow 1 \end{array}$$

where the composition  $\tilde{\pi} \circ s$  is surjective, since  $x_0 \equiv x_n \pmod{\tilde{R}F_{(2)}}$  and therefore  $G_S^T(2)$  is generated by the images of  $\tau_1, \dots, \tau_n$ . Clearly,  $\overline{R}$  is generated by  $\overline{r}_i = \psi(r_i)$ ,  $i = 1, \dots, n$ . By the assumptions made for the primes in  $S$ , we have  $r_i \in F_{(3)}$  and therefore also  $\overline{R} \subseteq \overline{F}_{(3)}$ . In particular, we obtain the *minimal* presentation

$$G_S^T(2) = \overline{F}/\overline{R} = \langle \overline{x}_1, \dots, \overline{x}_n \mid \overline{r}_1, \dots, \overline{r}_n \rangle$$

for  $G_S^T(2)$ . This yields  $h^1(G_S^T(2)) = n$ ,  $h^2(G_S^T(2)) \leq n$  and the cup-product  $H^1(G_S^T(2)) \times H^1(G_S^T(2)) \xrightarrow{\cup} H^2(G_S^T(2))$  is trivial, i.e. we have proven (i).

Next we calculate the triple Massey product of  $G_S^T(2)$ . Let  $\chi_0, \dots, \chi_n \in H^1(G_S(2)) = H^1(F)$  and  $\overline{\chi}_1, \dots, \overline{\chi}_n$  denote the bases dual to  $x_0, \dots, x_n$  and  $\overline{x}_1, \dots, \overline{x}_n$  respectively. Since  $\psi(x_0) \equiv \psi(x_n) = \overline{x}_n \pmod{F_{(2)}}$ , the inflation map  $\text{inf} : H^1(G_S^T(2)) \longrightarrow H^1(G_S(2))$  is given by

$$\overline{\chi}_i \longmapsto \chi_i, \quad i = 1, \dots, n-1, \quad \overline{\chi}_n \longmapsto \chi_0 + \chi_n.$$

Furthermore, we have the surjective homomorphism

$$\begin{aligned} \text{inf}^\vee : H^2(G_S(2))^\vee &\longrightarrow H^2(G_S^T(2))^\vee, \\ \text{tr}_{r_i} &\longmapsto \text{tr}_{\overline{r}_i}, \quad i = 1, \dots, n. \end{aligned}$$

Since Massey products commute with the inflation maps, for any  $1 \leq i, j, k, m \leq n$  we have

$$\begin{aligned} \text{tr}_{\overline{r}_m} \langle \overline{\chi}_i, \overline{\chi}_j, \overline{\chi}_k \rangle_3 &= \text{inf}^\vee(\text{tr}_{r_m} \langle \chi_i, \chi_j, \chi_k \rangle_3) \\ &= \text{tr}_{r_m} \text{inf}^\vee \langle \chi_i, \chi_j, \chi_k \rangle_3 \\ &= \text{tr}_{r_m} \langle \text{inf} \chi_i, \text{inf} \chi_j, \text{inf} \chi_k \rangle_3. \end{aligned}$$

We can now deduce (ii) by a direct calculation using 4.7 and the shuffle property of the triple Massey product.

Let  $H \subseteq G_S^T(2)$  be an open subgroup and  $k \subseteq \mathbb{Q}_S^T(2)$  the corresponding fixed field. Assume that  $H^{ab}$  is infinite. Since it is finitely generated, it has a quotient isomorphic to  $\mathbb{Z}_2$ . Assuming that the Leopoldt conjecture holds for  $k$  and 2, this must be the cyclotomic  $\mathbb{Z}_2$ -extension, since  $k$  is totally real (e.g. see [9], Th.10.3.6). However, the primes above  $q$  cannot be completely decomposed in the cyclotomic  $\mathbb{Z}_2$ -extension of  $k$  which yields a contradiction. Hence,  $H^{ab}$  is finite showing that  $G_S^T(2)$  is a *fab* group. In particular,  $(G_S^T(2))^{ab}$  is finite. Consequently  $h^2(G_S^T(2)) \geq h^1(G_S^T(2))$  and hence equality holds.  $\square$

**Example 5.3.** The sets  $S = \{2, 17, 7489, 15809\}$ ,  $T = \{5\}$  satisfy the assumptions made in 5.2. Choosing  $\overline{x}_i, \overline{r}_i, \overline{\chi}_i$  as in 5.2, computations of the Rédei

symbols with MAGMA show that

$$\begin{aligned}
 \text{tr}_{\bar{r}_1} \langle \bar{\chi}_i, \bar{\chi}_j, \bar{\chi}_k \rangle_3 \neq 0 &\Leftrightarrow (i, j, k) \in \{(1, 1, 3), (1, 2, 3), (1, 3, 2), (1, 3, 3), \\
 &\quad (2, 3, 1), (3, 1, 1), (3, 2, 1), (3, 3, 1)\}, \\
 \text{tr}_{\bar{r}_2} \langle \bar{\chi}_i, \bar{\chi}_j, \bar{\chi}_k \rangle_3 \neq 0 &\Leftrightarrow (i, j, k) \in \{(1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2)\}, \\
 \text{tr}_{\bar{r}_3} \langle \bar{\chi}_i, \bar{\chi}_j, \bar{\chi}_k \rangle_3 \neq 0 &\Leftrightarrow (i, j, k) \in \{(1, 1, 3), (1, 2, 3), (2, 1, 3), (3, 1, 1), \\
 &\quad (3, 1, 2), (3, 2, 1)\}.
 \end{aligned}$$

Hence, expressing the defining relations  $\bar{r}_1, \bar{r}_2, \bar{r}_3 \in R$  in the minimal presentation  $1 \rightarrow R \rightarrow F \rightarrow G_S^T(2) \rightarrow 1$  in terms of *basic commutators* of degree 3 using [12], Prop.1.3.3, we obtain

$$\begin{aligned}
 \bar{r}_1 &\equiv [[\bar{x}_1, \bar{x}_3], \bar{x}_1] [[\bar{x}_1, \bar{x}_3], \bar{x}_3] [[\bar{x}_2, \bar{x}_3], \bar{x}_1] \pmod{F_{(4)}} \\
 \bar{r}_2 &\equiv [[\bar{x}_1, \bar{x}_3], \bar{x}_2] \pmod{F_{(4)}}, \\
 \bar{r}_3 &\equiv [[\bar{x}_1, \bar{x}_3], \bar{x}_1] [[\bar{x}_1, \bar{x}_3], \bar{x}_2] [[\bar{x}_2, \bar{x}_3], \bar{x}_1] \pmod{F_{(4)}}.
 \end{aligned}$$

We claim that  $G_S^T(2)$  is mild. To this end let  $U = \langle \chi_1 \rangle$ ,  $V = \langle \chi_2, \chi_3 \rangle$ . By the above calculations the triple Massey product  $\langle \cdot, \cdot, \cdot \rangle_3$  is trivial on  $V \times V \times V$  and maps  $U \times V \times V$  surjectively onto  $H^2(G_S^T(2))$ . Hence, the mildness of  $G_S^T(2)$  follows by 2.8. Assuming the Leopoldt conjecture,  $G_S^T(2)$  is a fabulous pro-2-group.

To the author's knowledge, this yields the first known example of a fabulous pro- $p$ -group with trivial cup-product and also the first example of a fabulous pro- $p$ -group with generator rank  $\leq 3$ . J. Labute, C. Maire and J. Mináč have announced analogous results for odd  $p$ .

## REFERENCES

- [1] W. Bosma and J. Cannon. *Handbook of Magma functions*. School of Mathematics and Statistics, University of Sydney, 1996.
- [2] J. Gärtner. Higher Massey products in the cohomology of mild pro- $p$ -groups. *preprint*, 2012.
- [3] H. Koch. *Galois Theory of  $p$ -Extensions*. Springer, 2002.
- [4] M. Kolster. The 2-part of the narrow class group of a quadratic number field. *Ann. Sci. Math. Québec*, 29, no. 1:73–96, 2005.
- [5] D. Kraines. Massey higher products. *Trans. Amer. Math. Soc.*, 124:431–449, 1966.
- [6] R. Kučera. On the parity of the class number of a biquadratic field. *J. Number Theory*, 52:43–52, 1995.
- [7] J. Labute. Mild pro- $p$ -groups and Galois groups of  $p$ -extensions of  $\mathbb{Q}$ . *J. reine u. angew. Mathematik*, 596:155–182, 2006.
- [8] M. Morishita. Milnor invariants and Massey products for prime numbers. *Compositio Math.*, 140:69–83, 2004.
- [9] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*, 2nd edition. Springer, 2008.
- [10] L. Rédei. Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I. *J. reine u. angew. Mathematik*, 180:1–43, 1938.
- [11] A. Schmidt. Über Pro- $p$ -Fundamentalgruppen markierter arithmetischer Kurven. *J. reine u. angew. Mathematik*, 640:203–235, 2010.
- [12] D. Vogel. *Massey products in the Galois cohomology of number fields*. PhD thesis, Universität Heidelberg, 2004.

- [13] D. Vogel. On the Galois group of 2-extensions with restricted ramification. *J. reine u. angew. Mathematik*, 581:117–150, 2005.

Mathematisches Institut  
Universität Heidelberg  
Im Neuenheimer Feld 288  
69120 Heidelberg  
Germany

e-mail: gaertner@mathi.uni-heidelberg.de